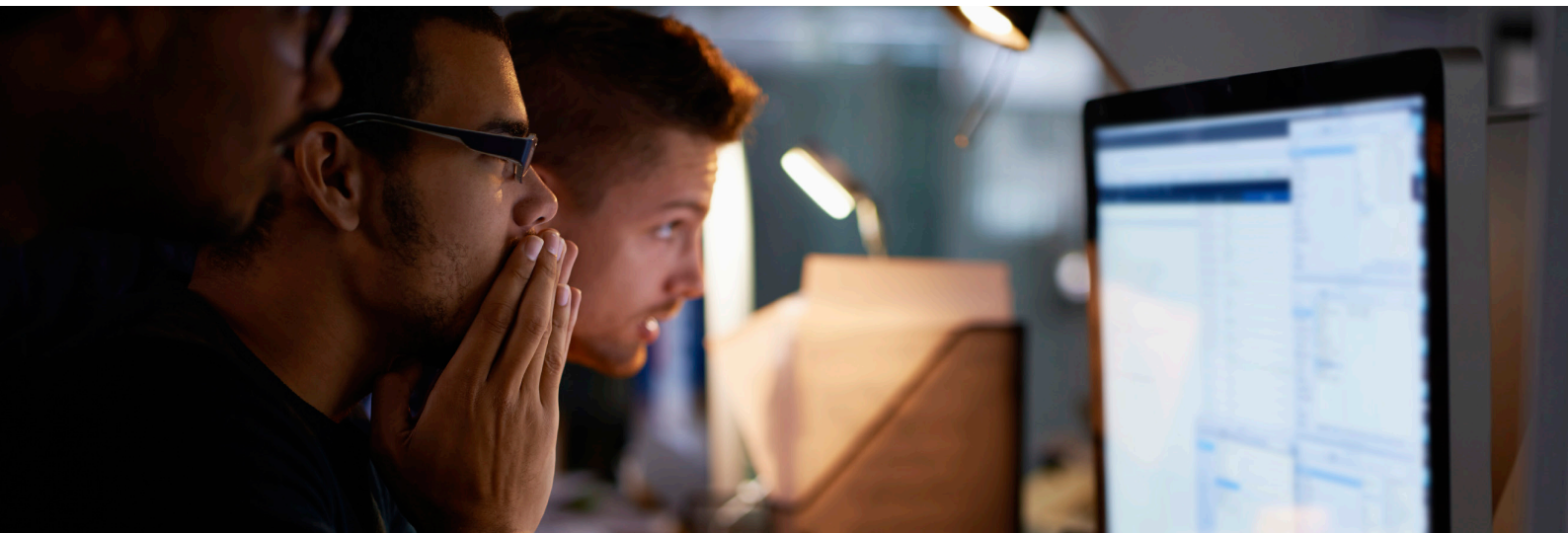




# Firewall Migration Methodology

Juniper SRX





## Introduction

The purpose of this document is to outline the methodology or “Method of Procedure” used by the Professional Services team when delivering a migration service from a Juniper SRX to a FortiGate configuration. The phases included in this document would be applicable to any third-party firewall, however, the aim is to highlight specifics for a Juniper SRX migration, as this is the principle migration request, from our customer base.

This document is designed for Customer’s Security Teams (Engineering, Implementation or Support) to facilitate the preparation of a firewall migration. It should be noted it is not a Scope of Work, nor should it be used as a Network Implementation Plan which requires detailed actions and planning.

The high level phases when planning any firewall migration are;

- Assessment & Requirements Analysis
- Planning, Architecture & Conversion
- Migration & Implementation

## Assumptions

This document cannot cover all deployment scenarios therefore a list of assumptions is outlined below.

### Elements in scope

- Firewalls operating in firewall-only/NAT/Router mode.

### Elements not in scope

- A re-design of the existing architecture
- Application Layer Gateway (SIP, GTP, etc) and related activities
- Introduction of new features and functionality
- Migration of UTM services
- VPN client migration
- FortiManager and FortiAnalyzer or any other network or system integration

It should be noted that the migration of IPSEC VPNs requires a thorough design review and requires the development of a migration plan (based on a “one shot” or “phased” migration), which takes into consideration all potential risks, for example, interoperability with third party products and resource capacity.

## Architectural Considerations

The Juniper SRX firewall security architecture is partially based on NetScreen's ScreenOS design, however, it utilizes the Juniper JunOS common shared code base. This code base has been re-used to implement routing daemons and other control plane functions, which are common, to a variety of routing and switching devices produced by Juniper. The forwarding and data plane functions are implemented separately for each SRX hardware platform.

The SRX and FortiGate firewalls are "Zone" based, but in the case of Juniper SRX, a logical interface must be assigned to a security zone. The security zone is a fundamental building block of the Juniper SRX architecture. In FortiOS case zones are optional which provides more flexibility for FortiOS configurations.

Juniper SRX implements the NAT function via NAT policies which are separate from firewall policies, and, NAT policies are not directly bound to interfaces. FortiOS, on the other hand, uses NAT policies which are explicitly bound to network interface which allows for more optimal processing. In order to effectively convert SRX NAT policies to FortiOS NAT policies, it is necessary to be aware of the translation order for source/destination NAT, and its interaction, with firewall policies on SRX platforms.

On the Juniper SRX firewall virtualization is realized via Routing Instances (routing-instances) and Logical Systems (logical-systems). A FortiOS VDOM roughly corresponds to the Juniper SRX logical-systems feature. The Juniper SRX Routing Instance is a collection of routing tables with associated interfaces. This can lead to complex configurations, and non-trivial interactions between routing instances, due to the fact that JunOS shares its code base among all router/switch/SRX platforms which means that certain design methodologies which are specific to another appliance type such as router, are implemented in the SRX firewall.

Juniper SRX High Availability is achieved with Chassis Cluster which forms one logical firewall from two SRX physical devices. The numbering of the interfaces on the cluster is contiguous; it starts on the first physical unit and continues on the second physical unit. This needs to be taken into account during a migration to a Fortigate HA cluster which keeps the interface numbering scheme intact.

With the help of tools to facilitate a configuration conversion, Professional Services utilize a strict methodology and work closely with customer Security Administrators to help decide upon the optimal approach to enable a successful migration.

## Assessment & Requirements Analysis

The purpose of this phase is to define the project baseline and ensure a clear understanding of the requirements and objectives of the project.

The first step in the process is for the customer to provide the existing configuration as well as a checklist of configuration and design elements. The checklist is aimed to review in particular:

- Objects & Groups, Nested Groups
- Policies
- Routing
- Interfaces
- Monitoring and Logging

A thorough review of the existing configuration is best practice before commencing any firewall migration, firstly to ensure an in-depth understanding of the environment, but also to identify areas for improvement in the logic of the rule base.

A firewall migration is also an opportunity for the customer to optimize the existing configuration. After many years of service, the rule set of a firewall can often become over-complex, some common examples of reasons for this are;

- Administrators prefer to add a new rule rather than editing an existing one
- Rules and objects can become obsolete because a service was decommissioned but the corresponding rule remains in the database
- There is no comment associated to the rule to understand its purpose or validity
- Over time a firewall can be managed by different technicians who do not follow the same implementation guidelines

To perform an initial optimization of the existing configuration, it is possible to use a conversion tool, however, at this stage a manual review and verification from the customer's security experts is required. It should be noted that based on field experience these two actions of configuration clean up, and, initial optimization can significantly reduce:

- The time allocated to the conversion and configuration review phase
- The number of policies active on the new system
- The number of conversion errors uncovered during the implementation and monitoring phase

Once the initial phase has been completed the migration kick-off meeting can take place, the key objectives of which, are to:

- Define requirements, project objectives and timing
- Discuss the checklist of configuration and design elements
- Discuss the conceptual differences between a FortiGate and Juniper SRX firewall
- Discuss the optimization of the existing configuration

At the end of this phase an agreement should be reached on the key elements of the migration planning which are; Project Timelines, High Level Design concepts and Optimization objectives. This ensures that when the configuration migration is complete, the new firewall rule set is documented and clearly understood by all parties.


A key action at this moment will be for the customer to implement a network freeze, whilst the target configuration is prepared and verified for deployment

## Planning, Architecture & Conversion

### FortiConverter

Fortinet has invested in the creation of a number of internal tools to facilitate the conversion of configuration files, in particular a tool called FortiConverter. The purpose of this application is to assist in the conversion of configurations from third party firewalls.

FIGURE 1: FORTICONVERTOR



Support Platform	
Platform	Version
Cisco router	IOS 10.x, IOS 11.x, IOS 12.x
Cisco PIX/ASA	Pix 4.x, Pix 5.x, Pix 6.x, Pix 7.x, Pix 8.x
Checkpoint	Smart Center, Provider-1 (excluding VPN-1 Edge, Safe@Office, SMP), with OS NG FP1 (4.0) to NGX R65 (6.5)
Juniper	ssg with OS 5.x

Support Feature				
	Cisco router	Cisco PIX	Checkpoint	Juniper
Policy	✓	✓	✓	✓
Object	✓	✓	✓	✓
Static route	✓	✓	✗	✓
Service	✓	✓	✓	✓
NAT	✓	✓	✓	✓
VPN	✓	✓	✓	✓

### Rule Set Translation

Once the configuration has been processed by the FortiConverter application it will still require manual verification. The amount of manual work required is dependent on the complexity of the rule set to be migrated. This process may be more onerous if the original rule set was not optimized, in particular with respect to the review of all Network Address Translation Rules and “Any” policies.

At this stage the active participation of the customer is will be required, to provide additional explanations of individual rule sets. The consultant will also request “read-only” access to the firewall to be migrated at the customer site through SmartDashBoard and SmartViewTracker.

### Configuration Pre-Staging

Once the rule set has been translated the consultant will load the configuration onto a test firewall in the FortiLabs to perform verification and testing. Once complete, details such as the routing tables are integrated. This will allow the full configuration to be prepared to a production standard before it is loaded onto the target firewall at the customer site.

The new firewall is therefore running the candidate configuration in order that the customer and Fortinet can access the device through the management network. This allows if required or feasible local testing of critical network applications.

### Configuration Review

At this point in the project there is a full joint review of the proposed final configuration to ensure firstly, a final agreement, but also to provide a final opportunity for any additional clean-up of the rule base.

### Product Knowledge Transfer

The Professional Services consultant will use the configuration review meeting to provide a Knowledge Transfer on the details of the configuration design, the logic and strategy of the rule sets and if required specifics of the hardware platforms utilized for the solution.

## Migration & Implementation

This phase corresponds to the day when the migration will take place and the legacy Juniper firewall is decommissioned.

### Pre-cutover Verifications

Prior to the service activation the customer is requested to run a series of tests to baseline the 'solution' before the migration. This step is achieved by:

- Writing scripts to test connectivity and service availability to critical resources. For example can end-stations can reach the internet, is mail is sent and received from designated mail servers.
- Writing test procedures to verify service availability.

Example test procedures:

- Can the mail server resolve against its DNS servers?
- Can a client send/receive emails?
- Are web servers able to reconnect to their database?
- Are the servers in the DMZ reachable from the Internet?

The customer is responsible for the creation of these procedures and scripts as they relate to their infrastructure and application base. It is also recommended that the security, server, and data networking teams take place in this activity to create a comprehensive snapshot of critical systems. Once the baseline is complete and recorded, it is possible to start the migration to the new solution.

### Cutover

The legacy system is decommissioned and the FortiGate activated.

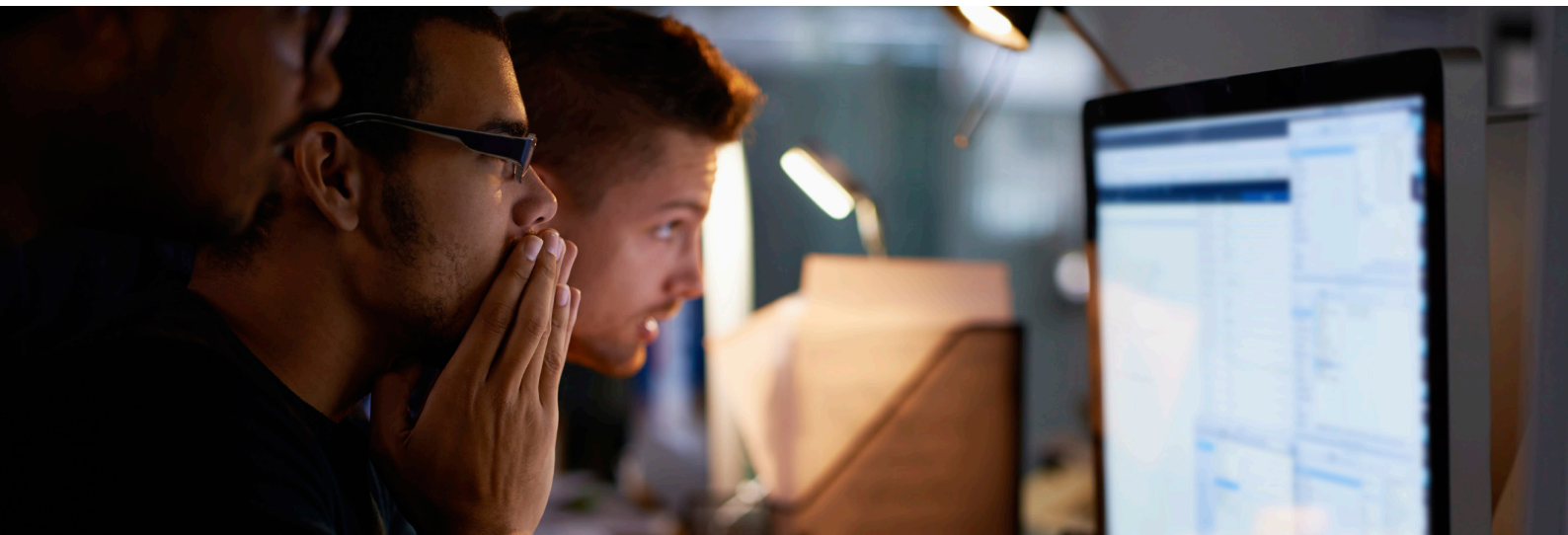
The Professional Services consultant performs a sanity check to ensure traffic is passed through the new firewall and that the system is behaving correctly. Once complete the customer is requested to perform a post-cutover validation.

### Post-cutover Validation

The customer runs the baseline scripts and procedures, as performed during the "pre-cutover verification" phase. If required analysis is performed and configuration adjustments created in order to resolve any specific connectivity issues.

### Acceptance

Once the validation phase is successful, the system remains in production. During a pre-agreed monitoring period (usually set to 15 calendar days), the customer may contact the Fortinet consultant to request assistance in resolving any connectivity issue directly related to the migration.



## Migrating a complete Firewall infrastructure

If a customer has a requirement for a complete migration of their firewall infrastructure the first step would be to understand both the overall network design as well as any pre-defined project planning. With this information the consultant could start building a migration strategy with the customer to mitigate risk as well as ensure operational effectiveness for the project duration.

Although each customer environment is unique, in general the following approaches are typical for a large migration;

- Perform initial migrations in non-critical areas as a test exercise. This builds confidence in the solution as well as Fortinet skill sets within the customer as well as identifying any requirements for specific application handling. Some examples are firewalls deployed in non-critical areas such as general office deployments or a Disaster Recovery location.
- Parallel migrations whereby the legacy and FortiGate system is in operation for a period of time. This allows for full redundancy as well as allowing operational effectiveness to be built up over time.
- In the core of the network it may be feasible to migrate individual VDOMs or Virtual Firewalls individually to minimize the risk of “one-shot” firewall migration.
- If the customer has very specific functionality the migration can be performed depending on the service requirement. This is typical in a telecommunications environment, where firewalls may be dedicated to functionality such as GTP.



---

[www.fortinet.com](http://www.fortinet.com)

GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 Kifer Road  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

EMEA SALES OFFICE  
120 rue Albert Caquot  
06560, Sophia Antipolis,  
France  
Tel: +33.4.8987.0510

APAC SALES OFFICE  
300 Beach Road 20-01  
The Concourse  
Singapore 199555  
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE  
Prol. Paseo de la Reforma 115 Int. 702  
Col. Lomas de Santa Fe,  
C.P. 01219  
Del. Alvaro Obregón  
México D.F.  
Tel: 011-52-(55) 5524-8480